SUPPLEMENTAL FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING MOTION TO DISMISS FOR SPOLIATION OF EVIDENCE

BACKGROUND

Seth Allen Aikens, II ("Mr. Aikens") was named in a superseding indictment with counts 1 through 17 for wire fraud, counts 18 through 24 for mail fraud, and counts 25 through 30 for money laundering. Mr. Aikens has entered a plea of NOT GUILTY.

On May 2, 2025, this Court conducted an evidentiary hearing on Mr. Aikens's Motion to Dismiss for Spoliation of Evidence.[1] The Court ordered both parties to file Findings of Fact and Conclusions of Law relative to the motion.[2] This brief follows that directive and incorporates the crucial testimony and evidence presented at the hearing.

The Government's Theory vs. Reality

This case presents the most egregious example of government evidence destruction in the digital age, compounded by a systematic pattern of deception that prevented timely discovery of the destruction. The Government proclaims to want to prove its theory on financial transactions, but this rings hollow when they have systematically destroyed or lost access to evidence showing what those transactions actually purchased. They point to payments received while rendering invisible the actual work product those payments compensated for.

This prosecution exemplifies the danger of prosecutorial tunnel vision. Rather than investigating whether fraud actually occurred, the Government appears to have decided on guilt first and then sought to construct a case by avoiding evidence that would contradict their predetermined conclusion.

Mr. Aikens's Reasonable Reliance and the Shocking Discovery

Until late 2024, Mr. Aikens operated under the reasonable assumption—created by the Government's own representatives—that they possessed the seized passwords and the binder/USB and could access the encrypted devices. When Mr. Aikens received the updated evidence spreadsheet toward the end of 2024, showing significant separation from the Government's official record and the transcript from the withdrawal hearing, he concluded the Government had somehow corrupted file headers or damaged the devices during their examination attempts.

Mr. Aikens's technical knowledge led him to assume the Government had damaged the devices through improper handling—perhaps corrupting file systems during examination attempts.

Only when Mr. Aikens actually asked HSI investigators to see the actual papers or looking for the responsive binder did they reveal the shocking truth: they only had a few scattered passwords, no silver binder existed in their custody, and Mr. Aikens noted to counsel "Hey look, no 3rd binder." This revelation transformed the case from suspected technical corruption to confirmed comprehensive evidence destruction or loss none of which has been explained.

FINDINGS OF FACT

A. The May 24, 2022 Seizure and Immediate Protocol Violations

1. Powered-On Systems and Mandatory RAM Capture Requirements

On May 24, 2022, federal agents including Special Agent David Coleman (HSI), Special Agent Scott Fell (HSI), and (USPIS) Inspector Gealey executed search warrants at Mr. Aikens's residence. As Mr. Aikens testified at the May 2, 2025 hearing: "The computers were on in the house, all three of the computers."[3]

This critical fact is corroborated by the Government's own search warrant photos (Exhibits 34-37 to Doc. 70), which show illuminated LEDs, active displays, and other

clear indicators of running systems. When computers are running with encrypted volumes mounted, the decryption keys exist in volatile memory (RAM) and vanish irreversibly the moment power is lost.

Federal agents receive mandatory training at the Federal Law Enforcement Training Centers (FLETC) Digital Forensics Examiner Program, which explicitly states: "Students will conduct RAM capture analysis."[4] The FLETC training description makes clear this is a fundamental requirement taught to all federal digital forensics personnel.[5]

2. Government Witness Testimony Reveals Unexplained Decision-Making and Avoided Liability Questions

Neither the Government's digital forensics team member David Coleman nor consulting team member Joseph Soeka addressed the fundamental question of who bore liability for the critical decision to destroy volatile evidence by powering down running systems. Both witnesses conspicuously avoided examining the decision-making process that led to immediate evidence destruction.

Coleman's testimony presents a significant contradiction. He collected password documentation that clearly articulated device names and corresponding passwords, indicating he reviewed this material before confidently proceeding to shut down the systems. The existence of password documentation suggests there was no urgent need to immediately power down the devices, as the notation indicated encrypted systems that could be accessed later with proper credentials.

If Coleman was indeed "confident" in his assertions about the encryption state and the impossibility of data recovery without passwords, he must have examined materials that clearly articulated computer-name-to-key relationships before someone authorized the destruction of volatile evidence by powering down active systems. The absence of such review would render Coleman's confident assertions about encryption and accessibility completely unfounded. See Exhibit 12.

Coleman's ability to access the gaming computer and his confidence in shutting down powered systems suggests the Government possessed exactly the passwords needed for access while simultaneously claiming impossibility of access. This contradiction undermines the credibility of the Government's position regarding data accessibility.

Similarly, Senior Digital Investigative Analyst Joseph Soeka's April 30, 2025 response entirely sidesteps the liability question. While Soeka addresses various technical matters, he completely fails to address whether proper protocols were followed in making the power-down determination at the scene, or **who bore responsibility for the decision to destroy active systems containing encrypted data.**

Soeka conspicuously avoids addressing the fundamental question of decision-making authority: whether anyone with supervisory responsibility evaluated the specific circumstances at the scene, reviewed the available password documentation, or followed established protocols before authorizing the destruction of volatile evidence by powering down active systems. This silence is particularly troubling given that Soeka appears to have had no direct involvement or knowledge of the scene, recovery, devices or "cracking" processes. The record strongly suggests that Soeka and Coleman operated independently without meaningful collaboration, rendering Soeka's after-the-fact technical review superficial at best.

B. The Government's Three-Tier Password System Destruction

1. Government's Selective Success Proves Password Possession

Evidence emerged during cross-examination. When prosecutor Melucci asked about wanting to come to HSI offices, Mr. Aikens testified: "Well, the computer that's turned on in the search warrant photos, the right one, the gaming computer, you guys had turned that over in discovery."[12]

This testimony reveals that the Government successfully accessed "the gaming computer" using the seized passwords, proving both that the passwords worked and that the Government possessed them. Yet they simultaneously claimed inability to access other encrypted devices while possessing the same password materials.

This selective success destroys any claim that the passwords were ineffective or that the Government lacked access to them.

2. Government's Comprehensive Control Over All Decryption Materials

The Government possessed complete control over a sophisticated decryption system:

Comprehensive Password Documentation: Official seizure logs document separate password sheets providing written backup of all system access credentials.

Digital Password Backup System: A USB drive containing plaintext versions of all passwords, providing immediate digital access without requiring physical papers.

Live System Access: An active computer system with logged-in password manager providing real-time access to all encryption keys, which they destroyed by powering down rather than performing standard RAM dump procedures which a federal forensic agent agreed and confidently shut down by clearly having those passwords like Exhibit 12.

3. Technical Claims Contradicted by Facts

Regarding the 2011 MacBook containing years of business evidence, Mr. Aikens testified: "It shouldn't be encrypted. It's from 2011. That's premature for what's called 'file vault,' and that's Apple's form of encryption."[13] This device predates standard encryption protocols, yet the Government claims inaccessibility while the hard drive appears to have been physically lost or destroyed. Only did file vault 2 introduce full disk encryption.

C. Mr. Aikens's Reasonable Reliance on Government Representations

1. The "Ongoing Forensic Review" Fiction (2022-2024)

For over two years, Mr. Aikens reasonably relied on the Government's explicit representations about ongoing forensic examination:

July 26, 2022: AUSA Gregory Melucci wrote: "I believe that covers the Rule 16 material in our possession, except forensic review results of electronic devices. We can provide that to you upon completion."[14]

February 21, 2024: AUSA Melucci told this Court: "That may take 45 to 60 days to get those completely forensically examined, of course. And we'll turn those results over to defense counsel, whomever that may be, promptly."[15]

These representations created reasonable reliance that:

- Forensic examination was proceeding normally
- Results would be provided upon completion
- The Government possessed working passwords
- Technical delays explained the extended timeline

2. Mr. Aikens's Technical Assumptions About File Corruption

The government has represented to this Court that no additional discoverable or producible material exists, placing the Court in the untenable position of relying on speculation rather than evidence. The record lacks essential details regarding the forensic examination process, creating significant evidentiary gaps that undermine the integrity of the digital evidence.

Critical Missing Documentation

The government has failed to provide fundamental information about their forensic examination, including the identity of personnel who performed the device examination, whether the examination was conducted on original devices or forensic mirrors, the

specific methodologies employed, the timing and location of the examination, and the rationale for attempting to crack devices when the government admittedly possessed the passwords (See Exhibit 12). If forensic mirrors were created, the government has produced no evidence of their existence or current location.

Contradictory Evidence Regarding Device Images

HSI Agent Scott Fell indicated in correspondence to current counsel that the government possessed duplicative images of the devices. However, the current location and status of these images remains wholly unaccounted for in the government's productions. This evidentiary gap substantially supports the defense's request for access to at least the MacBook image, particularly given that the device has now inexplicably lost its hard drive.

The Court should note an apparent contradiction in the government's position: during Agent Fell's interview with Scott Rayback, Mr. Rayback stated that a MacBook was never used. This inconsistency, coupled with the convenient disappearance of the hard drive containing case relevant data, raises serious questions about the government's handling of digital evidence.

Mr. Aikens's Reasonable Technical Conclusions

Prior to the HSI meeting, Mr. Aikens reasonably concluded—based on his technical expertise—that the government had corrupted file headers or similar technical elements during their examination attempts. This belief was reinforced when Mr. Aikens received an updated spreadsheet near the end of 2024 showing significant discrepancies from the government's official representations.

Given the technical reality that passwords should provide immediate access, the government's claims of ongoing review always made no sense.

3. The 26-Month Documentation Void

For nearly two years, the Government maintained their forensic review fiction without any documented activity.

The record reveals complete absence of:

- Forensic examination reports
- Tool logs or software output
- Laboratory submission forms
- Progress documentation
- Time tracking for examination efforts

This documentation void spanning 26 months proves no genuine forensic examination was attempted until forced by Court inquiry.

D. The Late 2024 Discovery: Evidence of Corruption or Destruction

1. The Updated Spreadsheet and Separation from Official Record

When Mr. Aikens received the updated spreadsheet toward the end of 2024, it revealed significant discrepancies between what the Government had officially represented and the actual status of evidence examination. These discrepancies created reasonable suspicion that something had gone wrong with the devices themselves.

2. Agent Fell's Contradictory Statements

Agent Fell had told current counsel that the Government obviously had the originals and working copies. However, the complete absence of any chain of custody documentation, proof of images and no MacBook image contradicted these representations, leading Mr. Aikens to conclude the Government had somehow corrupted or damaged the devices during improper examination attempts.

3. Technical Impossibilities in Government Claims

Mr. Aikens's technical expertise revealed fundamental contradictions in the Government's representations:

The Government's claims defied basic principles of digital security. Either the devices were properly encrypted with passwords—in which case access would be immediate upon entering the correct credentials—or they were not, making access genuinely impossible without those credentials. Modern encryption algorithms used in standard devices cannot be defeated by "sophisticated cracking tools" when properly implemented, a fact the Government acknowledged in its subsequent response.

The Government's shifting timeline and explanations created a pattern of technical impossibilities. Their representations suggested they possessed both the capability to access encrypted devices and simultaneously lacked such capability, depending on the procedural posture of the case.

Given these irreconcilable technical contradictions, Mr. Aikens reasonably concluded that the Government had damaged the devices or the like. The Government's technical assertions simply could not coexist with established principles of digital forensics and encryption technology.

E. The HSI Meeting Revelations: Complete Evidence Destruction

Following this Court's explicit guidance at the May 2, 2025 hearing, Mr. Aikens demonstrated good faith cooperation by agreeing to meet with HSI agents. The Court had observed: "I think maybe accepting the Government's invitation to meet might actually kind of break through that impasse."[16] See Exhibit 60.

1. The Responsive Silver Binder Has Completely Vanished

The Government's production of password documentation revealed both evidentiary mishandling and exonerating evidence. When Mr. Aikens requested to examine the "papers listing passwords" that Agent Coleman had specifically logged as seized

property, the Government produced only a small packet of papers—a fraction of what was documented as seized.

The passwords contained in this limited production were functional and led to real accounts that could be successfully accessed. Crucially, examination of these accounts demonstrated no criminality whatsoever, directly contradicting the Government's allegations. However, these accounts are meaningless to this case and contain non-responsive data unlike Exhibit 12 and it's like papers, the missing pages are what have contained encryption keys and other passwords directly relevant to the devices and allegations at issue.

Meanwhile, the Government does possess two other silver binders, but these containers have been stripped of virtually all contents. One binder shows visible damage to its clasp mechanism, suggesting mishandling during Government custody.

As Mr. Aikens observed to counsel: "Hey look, no 3rd binder." The stark disparity between what was documented as seized and what was ultimately produced suggests that substantial password documentation was destroyed or lost through gross negligence. The Government appears to have preserved only the irrelevant passwords while losing the very encryption keys and passwords that would have been responsive to their investigation and exonerating Mr. Aikens.

2. Critical Passwords Selectively Destroyed

Of the thirty-one documented passwords papers that should have been in the binder, the Government could produce only a handful. The specific passwords for encrypted containers and like cloud accounts containing exculpatory evidence? Gone.

This selective destruction cannot be explained by innocent negligence. If an entire binder were misplaced, all passwords would be missing. Instead, the most crucial passwords—those unlocking proof of innocence—have selectively disappeared while less important ones survived.

3. The USB Backup Device Has Disappeared

The USB device containing plaintext password exports—seized from the same safe and logged on the same evidence form—has vanished entirely. The Government provided no explanation for how a USB device disappears from federal evidence storage.

4. MacBook Missing Hard Drive & Signs of Improper Handling and Storage

The in-person examination (See Exhibit 60) revealed not merely technical problems but actual physical loss of evidence:

Mr. Aikens' first instruction to HSI and the Government was to power up the MacBook and demonstrate that it was requesting an encryption key. Agent Coleman attempted several approaches but after a few minutes could not access the device. Later in the meeting, before leaving, counsel requested to reexamine the MacBook since that portion of the inspection was incomplete. Coleman then randomly removed the back panel of the MacBook to examine, only to discover it was missing It's hard drive entirely while in custody. Notably, why didn't coleman run to get the forensic images agent fell claimed to counsel they have their own working copies? Did they never image any of these encrypted devices as backups incase the handling ever went wrong?

The examination revealed multiple signs of evidence mishandling. The MacBook's hard drive was completely absent from the device. The computer casing for another computer showed cracks from apparent dropping, markedly different from its condition in the search warrant photographs. All external hard drives displayed signs of improper handling and storage, appearing to have been carelessly thrown into boxes rather than properly preserved as evidence.

Most troubling was the complete absence of chain of custody documentation for any device. The Government could not account for when the hard drive went missing, who had access to the devices, or what procedures were followed to maintain evidence

integrity. This represented a fundamental failure of basic evidence preservation protocols that rendered the digital evidence worthless for prosecution purposes.

5. Agent Coleman's Damaging Admissions

Agent Coleman made two critical admissions that expose the government's misconduct. First, he acknowledged that in person "maybe they had a lot going on and something happened"—a stunning confession that federal agents were too distracted or overwhelmed to preserve vital evidence in this case he was specifically asked to join in.

More tellingly, Agent Coleman spontaneously introduced the concept of "kill switches" into the conversation—a topic that neither the defense nor Melucci had raised. This unprompted revelation demonstrates consciousness of guilt regarding evidence destruction or loss. The court should note carefully: it was Coleman himself, not the defense, not Melucci, but Coleman who brought up "kill switches," betraying his awareness.

These admissions collectively paint a picture of deliberate evidence destruction or loss disguised as bureaucratic negligence, with Agent Coleman's own words providing the most damaging testimony against the government's position.

F. Specific Exculpatory Evidence Lost Forever

The destroyed access prevents Mr. Aikens from proving his innocence in fraud allegations claiming he provided no legitimate services. The encrypted devices contain comprehensive proof of actual delivery across multiple business relationships:

1. Cherotti Enterprises: Complete Business Integration

Specific Evidence Lost (Doc. 70-1, p. 426):

- All email records for AvareSupply and Order Agreement
- Software Related to ZuRI Systems Connection

- Additional Phone Call Recordings
- Full Text Communications

This evidence would demonstrate the legitimate business relationship and actual software integration services provided to Cherotti Enterprises, directly contradicting fraud allegations.

2. Marco/PurestFormCBD: Comprehensive Inventory System

Specific Evidence Lost (Doc. 70-1, p. 426):

- Full Text Communications
- Entire Inventory Software and Log Backup and All Related Files
- Same Inventory System + Payment Processing as ZuRI

The Marco relationship involved the same sophisticated inventory system developed for ZuRI, proving systematic legitimate software development across multiple clients rather than fraudulent schemes.

3. Heartbeat Keepsakes/Meet Your Miracle: Application Development

Specific Evidence Lost (Doc. 70-1, p. 426):

- Original Mockup Application Ionic (First Recording Show App)
- Original Mockup Design Kit for Ionic
- Secondary PHP Application
- Original HBKS Website Backup .wpress/raw-dump/sql file
- Meet Your Miracle Peer JS Project Files
- Complete backup showing website security analysis
- In person recordings

This evidence demonstrates complete mobile application development including both iOS and Android versions, website development, and security consulting services.

4. ZuRI/Kaizen Systems: Core Business Development

Specific Evidence Lost (Doc. 70-1, pp. 426-427):

- 4 Backup files for The Original Website I built .wpress/sql/files
- Original Website backup from Aaron Cadena (previous developer's site)
- 2 Backup Files for Inventory System
- Additional In person recordings
- All files related to the "Mail Fraud" allegations showing Scott's approval of employee actions
- Sign off Sheets for All Work Done
- E01 Computer Image (Computer most of the work ZuRI was done on)

As documented: "Computer most of the work ZuRI Was done on, I took an E01 at the end and copied it to my drives." This represents complete forensic documentation of legitimate business operations that Mr. Aikens himself preserved in professional format.

5. Ryan Beichner: The Brute Cam Project

Specific Evidence Lost (Doc. 70-1, pp. 427-428):

- Brute Cam Build Project Files
- Brute Cam Design Files (Logo, AppScreens, Camos, etc.)
- Brute Cam Website Files (Front Facing for Sales)
- Brute Cam App Website Files (Backend for App to Connect)
- Brute Cam WhiteLabel Portal Files (E.g Cabelas or any Biz)
- Brute Cam Backend for Image Processing Files
- Brute Cam iOS Project Files
- Brute Cam Android project Files
- Evidence detailing the project timeline and work completed
- Server Logs

- All text messages
- Receipt for Repayment

This represents a complete trail camera system with sophisticated capabilities—exactly the opposite of a fraudulent scheme.

6. Erick Merryman: OBD and GPS Development

Specific Evidence Lost (Doc. 70-1, p. 428):

- Complete collection of files related to OBD reverse engineering and development
- Android application for Bluetooth lighting control
- Complete collection of files related to GPS Tracking & Customization
- Complete website and branding package
- Full source project files for the app, tailored with specific branding
- Evidence detailing the project timeline and work completed
- Server Logs
- Video of hand-delivering completion or not letter to Erick
- All text messages

7. Scott Andrus: Multiple Website Development

Specific Evidence Lost (Doc. 70-1, p. 428):

- CBD Website
- Saybrook Gardens Website
- Initial Versions of Apps
- Deployment Related Files
- All text messages

8. Tax and Corporate Documentation

Critical Business Records Lost (Doc. 70-1, p. 427):

- LLC Loan Agreements & Ledger for LLC to LLC loans
- Meeting Minutes for all LLCs taken

The Government seized all business tax folders, LLC boxes, and operating agreements from Mr. Aikens's safe, which documents apparently vanished, though digital copies remained on the now-inaccessible encrypted backups due to loss or destruction. Upon physical inspection, every LLC had no meeting minutes. No explanation, nothing.

G. Video and Audio Evidence of Legitimate Work Product

1. Attorney-Client Work Product Videos

The record contains extensive video documentation proving actual software development and delivery:

ZuRI System Demonstrations (Doc. 70-1, p. 427):

- [AttorneyClientWorkProduct] ZuRICBD - Web - Inventory - QuickBooks & Tax Integration (Ohio & PA Test).mp4
- [AttorneyClientWorkProduct] ZuRICBD - Web - Inventory Run - Through by Red Thread Tech.mp4
- [AttorneyClientWorkProduct] ZuRICBD & Kaizen - Payment Processing Plugin Test & Walkthrough.mp4

Mobile Application Demonstrations:

- [AttorneyClientWorkProduct] ManageZuRI - Android Demo by Red Thread Tech.mp4
- [AttorneyClientWorkProduct] ManageZuRI - iOS Demo by Red Thread Tech.mp4
- [AttorneyClientWorkProduct] ManageZuRI - Web Demo by Red Thread Tech.mp4

GPS Tracking System Demonstrations (Doc. 70-1, p. 428):

- [AttorneyClientWorkProduct] Ruff Bark Tracking - iOS Mobile WebView - Tracking Android Client 'Truck'.mp4
- [AttorneyClientWorkProduct] Ruff Bark Tracking - Web & Android Client Connecting to Web Manager.mp4
- [AttorneyClientWorkProduct] Ruff Bark Tracking - Web Truck Admin View Routes for GPS Recorded Travel.mp4

2. Comprehensive Application Portfolio

The destroyed evidence includes complete video demonstrations of functioning applications across multiple platforms:

E911 Emergency System:

- e911 - Android - App - Run-Through.mp4
- e911 - iOS - App - Run-Through.mp4
- Emergicare e911 w Spanish - Android App Run-Through.mp4
- Emergicare e911 w Spanish - iOS App Run-Through.mp4

Reservation and Booking Systems:

- ClickToReserve - Web - Admin - Run Through by Red Thread Tech.mp4
- ClickToReserve - Web - Admin - Run Through by Red Thread Tech - 2nd.mp4
- ClickToReserve - Titus Hill Signing Up - Booking and using user functions.mp4
- ClickToReserve - Web - Host Adding a Listing & Titus Viewing - Run Through by Red Thread Tech.mp4

Payment Processing Systems:

- PurestFormCBD - Payment Processing Plugin Test & Walkthrough.mp4

Lifestyle Applications:

- Heartbeat Keepsake - Run Through - iOS.mp4
- Heartbeat Keepsake - Run Through - Android.mp4

3. Audio Recordings with Clients

EXHIBIT A (Placeholder for Video Exhibit) // EXHIBIT B (Placeholder for Audio Exhibit) contained 2 audio recordings with actual conversations with Scott Raybuck & CO and Scott Andrus, providing direct client testimony about work performed and satisfaction with deliverables, showcasing performance of contracts.

4. Evidence Supporting Veracity of Claims

The record includes specific exhibits proving the existence and legitimacy of work at ECF 70-1 446 through 448:

- **Exhibit 039**: Evidence Supporting the Veracity of the Stated Claim - Proof of the 2 Backup files and All In One Backup on Desktop WITH the website open
- **Exhibit 040**: Evidence Supporting the Veracity of the Stated Claim - Sign Off Sheets Missing in relation to Government Seizure (Partly recovered a majority upon physical inspection but still missing some)
- **Exhibit 041**: Evidence Supporting the Veracity of the Stated Claim - Proof of Bulk Documents Missing
- **Exhibit 042**: Evidence Supporting the Veracity of the Stated Claim - Scott Raybucks confirms I did the work AT THE END

H. Missing Forensic Reports and Digital Evidence Problems

1. No Forensic Reports for Central Digital Evidence

Despite the central role of digital communications in the indictment, the defense has never been provided complete forensic reports for text messages mentioned in the charging document. Mr Aikens maintains he's not sure about the authenticity of the

alleged messages, but he maintains that his business records contain true forensic extractions with complete reports if he could access them which the record reflects.

2. Ryan Beichner's "Screenshot and Email" Methodology

In Beichner's communications with law enforcement, he merely took screenshots of messages and emailed them one by one, "losing his device" when comprehensive examination became relevant. This methodology:

- Prevents verification of message authenticity
- Eliminates metadata showing message context
- Allows selective presentation of communications
- Avoids forensic examination revealing complete conversation threads

3. Merryman's Wife's Phone: Missing Source Files and Technical Anomalies

The Government's forensic document regarding Merryman's wife's phone extraction revealed no "source file" for alleged messages. Suspicious technical anomalies include:

- Filename with two double spaces (unusual for automated systems)
- Window header cutoff suggesting screenshot rather than forensic extraction
- Presentation inconsistent with standard forensic reporting
- Literally shows no source file

4. Complete Absence of Victim Interview Documentation

Despite Government claims of complete discovery production, their files reveal only two brief interviews: Scott Raybuck and Cherroti Enterprises. No other victim interviews exist despite charging Mr. Aikens with allegedly defrauding customers involving approx. $1.3 million.[17] Raybuck acknowledges he *got his website*.

This glaring absence directly contradicts Government claims and raises serious questions about investigation adequacy.

I. Physical Damage and Complete Absence of Chain of Custody

1. Total Absence of Required Documentation

During the HSI meeting, Mr. Aikens discovered a complete absence of chain of custody documentation for any seized device. This means no record exists of:

- **Initial Seizure Documentation**: Who handled devices, packaging procedures, transportation
- **Custody Transfer Records**: Every person accessing devices, dates, times, purposes
- **Storage Documentation**: Environmental conditions, security measures, access logs
- **Examination Records**: Who attempted examination, tools used, results, authorization

We still don't know who handled what devices during crucial periods when evidence was being destroyed or lost. The Government has provided no documentation identifying which agents handled specific devices, who was responsible for password documentation, who attempted access, or who was present when devices were damaged.

2. The Missing MacBook Hard Drive: Years of Business Evidence Lost

As Mr. Aikens testified: [Actually Erick] "Erin and Ryan's projects are specifically on that MacBook."[18] This 2011 MacBook predates standard encryption yet the Government claims inaccessibility while the hard drive appears physically lost or destroyed. He also noted that backups *exist*.

This device contained years of client project files, business communications, and documentation of legitimate work establishing Mr. Aikens's innocence.

J. The Government's Inadequate Investigation

1. Failure to Subpoena Relevant Third-Party Evidence

The Government never sent subpoenas to companies such as InMotion Hosting, which served as Mr. Aikens's hosting provider for extended periods. This evidence would have provided independent, third-party verification of ongoing legitimate technical work that the Government chose not to pursue.

The subpoenas issued were deliberately limited in scope, seeking only "name, IP and basic" information rather than substantive technical data revealing reality of ongoing development work.

2. Avoiding Remote Servers Containing Proof of Work

The Government's systematic avoidance of remote server data represents the most telling aspect of their selective investigation. Modern web development relies heavily on cloud infrastructure. By failing to examine these systems, the Government ensured they would not discover evidence of working projects and legitimate deliverables.

APPLICABLE LAW

A. Foundational Spoliation Doctrine

1. Definition and Scope of Spoliation

Spoliation is defined as the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. *Paramount Pictures Corp. v. Davis*, 234 F.R.D. 102, 110 (E.D. Pa. 2005) (quoting *Mosaid Techs., Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 335 (D.N.J. 2004)). When spoliation occurs in criminal cases, the proper remedy is dismissal of the indictment. *United States v. Dudenhoefer*, No. 1:21-cr-39, 2025 U.S. Dist. LEXIS 4902, at *14 (W.D. Pa. Jan. 10, 2025).

2. Four-Element Spoliation Framework

As this Court has previously reasoned in *United States v. Miah*, No. 21-110, 2021 U.S. Dist. LEXIS 227689, at *7 (W.D. Pa. Nov. 29, 2021), in making a determination that spoliation of evidence occurred, a court must find that: "(1) the evidence was in the party's control; (2) the evidence is relevant to the claims or defenses in the case; (3) there has been actual suppression or withholding of evidence; and, (4) the duty to preserve the evidence was reasonably foreseeable to the party." *Bull v. UPS*, 665 F.3d 68, 73 (3d Cir. 2012) (citing *Brewer v. Quaker State Oil Refining Corp.*, 72 F.3d 326, 334 (3d Cir.1995)).

3. Sanctions Framework and Judicial Discretion

If Mr. Aikens demonstrates that evidence has been subject to spoliation, the Court may impose sanctions, such as the dismissal of a claim or claims, suppression of evidence, and/or an adverse inference. *Paramount Pictures Corp.*, 234 F.R.D. at 110-11. However, in exercising its discretion, the Court must consider the following factors: "(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party, and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future." *Id.* (quoting *Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994)).

4. Fault Analysis: Intent to Impair Litigation

Regarding the first factor--degree of fault--"the Court must consider whether [the party that destroyed the evidence] intended to impair the ability of the other side to effectively litigate its case." *Id.* (quoting *In re Wechsler*, 121 F. Supp. 2d 404, 415 (D. Del. 2000) (citing *Brewer v. Quaker State Oil Ref. Corp.*, 72 F.3d 326, 334 (3d Cir. 1995)).

5. Prejudice Analysis: Meaningful Opportunity Standard

With respect to the second factor, prejudice, "the Court should take into account whether [the party that did not destroy the evidence] had a meaningful opportunity to examine the evidence in question before it was destroyed." *Id.* at 112. In deciding on a sanction, the

Court should choose the "least onerous sanction corresponding to the willfulness of the destructive act and the prejudice suffered by the victim." *Id.* at 111; *United States v. Bunty*, 617 F. Supp. 2d 359, 370 (E.D. Pa. 2008).

B. Constitutional Protections and Government Obligations

1. Brady v. Maryland Mandatory Disclosure

The Supreme Court requires disclosure of evidence "favorable to an accused" that is "material either to guilt or to punishment." *Brady v. Maryland*, 373 U.S. 83, 87 (1963). The Government violates Brady by destroying access to exculpatory evidence while maintaining false representations about ongoing review.

2. Fifth Amendment Due Process

Due process prohibits governmental conduct that "shocks the conscience." *Rochin v. California*, 342 U.S. 165, 172 (1952). The Government's conduct clearly meets this standard through seizing evidence, destroying or losing access through gross negligence, lying about it for years, then proceeding to trial knowing defense is impossible.

3. Sixth Amendment Right to Present Defense

The Sixth Amendment guarantees the right to present a complete defense. *California v. Trombetta*, 467 U.S. 479, 485 (1984). This right becomes meaningless when the Government destroys access to evidence essential to that defense.

4. Arizona v. Youngblood Bad Faith Standard

Under *Arizona v. Youngblood*, "unless a criminal defendant can show bad faith on the part of the police, failure to preserve potentially useful evidence does not constitute a denial of due process of law." *Arizona v. Youngblood*, 488 U.S. 51, 58 (1988). The Supreme Court established that bad faith exists when "the police themselves, by their conduct, indicate that the evidence could form a basis for exonerating the defendant" and must be

determined based on "the police's knowledge of the exculpatory value of the evidence at the time it was lost or destroyed." *Id.* at 56-57.

C. Enhanced Federal Law Enforcement Standards

1. FLETC Training Requirements

Federal agents receive mandatory training at the Federal Law Enforcement Training Centers (FLETC) Digital Forensics Examiner Program, which explicitly requires "RAM capture analysis" and fundamental forensic techniques for preserving volatile evidence. *See* Digital Forensics Examiner Program, Federal Law Enforcement Training Centers, https://www.fletc.gov/digital-forensics-examiner-program. This training establishes mandatory protocols for powered systems, volatile data preservation before shutdown, chain of custody documentation, and recognition of exculpatory evidence. Again, Mr Coleman felt confident in his ability to turn off systems.

2. Professional Ethical Obligations

Government attorneys have heightened candor obligations as "servant[s] of the law" with duty to ensure "justice shall be done." *Berger v. United States*, 295 U.S. 78, 88 (1935). The Government's false representations about ongoing forensic review violate these fundamental obligations and undermine the adversarial system's foundational principles.

D. Enhanced Government Agency Obligations: Civil vs. Criminal Standards

1. Constitutional vs. Procedural Preservation Frameworks

Criminal prosecutions trigger immediate constitutional preservation duties upon investigation initiation that exponentially exceed civil litigation obligations. While civil cases involve procedural discovery rules, criminal prosecutions invoke constitutional mandates under Brady, due process, and the Sixth Amendment that create affirmative government obligations to preserve exculpatory evidence.

2. Heightened Standard for Government Agencies

The Middle District of Pennsylvania's decision in *Culler v. Shinseki* establishes enhanced preservation obligations for government agencies even in civil litigation contexts. *Culler v. Shinseki*, No. 1:09-CV-0794, 2010 WL 5387084 (M.D. Pa. Dec. 22, 2010). The *Culler* court emphasized that proper civil discovery requires "affirmative acts to prevent its system from routinely destroying information." *Id.* In criminal prosecutions, the Government operates under constitutional preservation mandates that far exceed civil litigation requirements.

3. Documented vs. Speculative Evidence Destruction

Unlike cases involving speculative harm from potential evidence loss, here Mr. Aikens has provided exhaustive documentation of precisely what evidence the Government destroyed, spanning multiple legitimate business relationships documented across Doc. 70-1, pages 426-428. The destroyed evidence includes technical documentation existing only in digital form: complete backups, server logs, forensic images, and proprietary source code. No witness testimony can recreate encrypted database backups or time-stamped computer forensic evidence, creating mathematical impossibility of reconstruction.

E. Judicial Estoppel Doctrine

Courts apply judicial estoppel to prevent parties from "prevailing in one phase of a case on an argument and then relying on a contradictory argument to prevail in another phase." *New Hampshire v. Maine*, 532 U.S. 742, 749 (2001). The doctrine prevents manipulation of the judicial system through contradictory positions that undermine judicial integrity and fairness to opposing parties.

F. Authentication and Chain of Custody Requirements

Melendez-Diaz v. Massachusetts established foundational principles regarding documentary evidence authentication in criminal prosecutions. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009). The complete absence of chain of custody documentation violates fundamental admissibility requirements and creates constitutional confrontation violations when defendants cannot examine evidence handlers or authenticate Government claims about evidence condition and handling procedures.

CONCLUSIONS OF LAW

A. All Spoliation Elements Conclusively Established

1. Government Control of Evidence (Element One)

From seizure on May 24, 2022, the Government exercised exclusive custody and control over all devices and password documentation. Unlike *United States v. Miah*, where this Court found the Government lacked control over rapidly changing Twitter content,[28] here the Government had complete physical custody with established protocols for preservation.

The May 2, 2025 hearing testimony conclusively established Government control:

Q. "How is that relevant for your argument today?"

A. "Because it states that they left the house with the papers listing passwords, the book documents, and the drives."[29]

The Government's own evidence recovery log documents seizure of "Book storage media and papers listing passwords, Room 0, Special Agent Coleman."[30]

2. Central Relevance in Fraud Prosecution (Element Two)

In a fraud case alleging Mr. Aikens provided no legitimate services, devices containing proof of actual delivery could not be more relevant. The May 2, 2025 hearing established specific exculpatory content:

Mr Melucci: "Can you tell Judge Hardy, generally if you recall, what's contained in the contents of those encrypted devices?"

Mr. Aikens: [Actually Erick] "Erin and Ryan's projects are specifically on that MacBook... Scott Raybuck's website, original backup from Aaron Cadena, all the files related to the Bluetooth lighting system, all the files relating to Brute Cam's iOS app, Android app, the original backup from Heartbeat Keepsakes, all the order agreements from Avare Supply, the full text message record from Ryan Beichner."[31]

This testimony, combined with the comprehensive documentation in Doc. 70-1 pages 426-428, establishes specific identification of exculpatory evidence across multiple business relationships.

3. Actual Suppression Through Physical Destruction (Element Three)

The May 2, 2025 hearing established both physical destruction and systematic concealment:

Physical Destruction:

- Silver binder with passwords: vanished from custody
- USB device: disappeared entirely
- Hard drive: physically missing from MacBook
- RAM keys: destroyed by improper shutdown

Government's Selective Success: The hearing revealed the Government successfully accessed "the gaming computer" using seized passwords while claiming inability to access other devices containing exculpatory evidence.[32]

Systematic Concealment: Two years of false "ongoing review" claims with no documented examination attempts.

4. Obvious Duty to Preserve (Element Four)

The Government's preservation duty was constitutionally mandated. Federal agents had Brady obligations, mandatory FLETC training, professional awareness of exculpatory value, and official documentation of password seizure.

As this Court recognized during the hearing:

THE COURT: "Are you contending that that's a constitutional violation?"

MR. WALKER: "Yes, Your Honor."

THE COURT: "Fourth Amendment in particular?"

MR. WALKER: "Yes, Your Honor, and also Fifth Amendment by due process, Your Honor."[33]

B. Constitutional Violations Requiring Dismissal

1. Brady Violation Through Systematic Destruction and Concealment

The Government's conduct represents the most egregious possible Brady violation: destroying access to exculpatory evidence while promising disclosure "upon completion." They didn't merely fail to disclose--they affirmatively destroyed Mr. Aikens's ability to access evidence proving innocence while maintaining a fiction of ongoing examination.

The May 2, 2025 hearing revealed the Government successfully used seized passwords to access some devices while claiming universal inaccessibility--selective suppression designed to prevent Mr. Aikens from proving innocence.

2. Due Process Violations Under Rochin Standard

The Government's conduct shocks the conscience through seizing evidence, destroying access through gross negligence, lying about examination status for over two years, blaming Mr. Aikens for inaccessibility they created, and proceeding to trial knowing defense is impossible.

3. Arizona v. Youngblood Bad Faith Standard: Government's Documented Knowledge of Exculpatory Value

Under *Arizona v. Youngblood*, "unless a criminal defendant can show bad faith on the part of the police, failure to preserve potentially useful evidence does not constitute a denial of due process of law." The Supreme Court established that bad faith exists when "the police themselves, by their conduct, indicate that the evidence could form a basis for exonerating the defendant" and must be determined based on "the police's knowledge of the exculpatory value of the evidence at the time it was lost or destroyed."

a. The Government's Own Investigation Documents Actual Service Delivery

The Government's conduct here far exceeds *Youngblood*'s bad faith threshold because their own grand jury presentation conclusively establishes knowledge of exculpatory value from the investigation's inception. In describing the Scott Raybuck (ZuRI CBD) allegations, the Government's presentation explicitly acknowledges actual service delivery:

"Received some IT services promised but no tangible/software items provided. For example, website was produced but no inventory system or labeler machine." Grand Jury Presentation at 26, ECF No. 67-1 (emphasis added).

This admission destroys any claim that the Government lacked knowledge of exculpatory value. They knew from the investigation's beginning that Mr. Aikens actually delivered working websites and IT services--directly contradicting their fraud theory that "no legitimate services" were provided. The destroyed encrypted devices containing

comprehensive proof of legitimate work product across multiple clients would demonstrate a systematic pattern of actual delivery rather than fraudulent schemes.

b. Multiple Categories of Knowing Misconduct

The Government's bad faith manifests through several interconnected categories of deliberate misconduct:

Selective Evidence Destruction with Knowledge of Exculpatory Value: The May 2, 2025 hearing established that federal agents successfully accessed the gaming computer using seized passwords while simultaneously claiming universal device inaccessibility. This selective suppression occurred while the Government possessed documentation in their own files acknowledging actual service delivery, proving they knew the encrypted devices would contain evidence of legitimate work product.

Consciousness of Guilt Through "Kill Switch" Discussions: Agent Coleman's spontaneous introduction of "kill switch" discussions in the initial briefing reveals awareness that evidence was deliberately destroyed rather than lost through negligence. Neither defense counsel nor prosecutors had raised deliberate destruction mechanisms, yet Coleman immediately brought up while misleading about "Bitlocker" being somehow different AES 256 that it uses, intentional elimination methods, betraying consciousness that the evidence destruction was calculated misconduct rather than technical failure.

Systematic Deception to Conceal Destruction: The Government compounded this bad faith through sustained misrepresentation spanning over two years, falsely claiming ongoing forensic examination while maintaining no documentation of any examination attempts. This deliberate concealment prevented timely discovery of evidence destruction and demonstrates the calculated nature of their conduct. It also prevented timely motion practice and candor to the Court.

Violation of Mandatory Professional Protocols: Federal agents violated explicit FLETC training requirements by destroying volatile RAM evidence on powered systems,

directly contravening their professional obligations. This cannot be characterized as mere negligence when agents receive mandatory training specifically requiring RAM capture on powered systems.

c. Exceeding Youngblood's Bad Faith Threshold

Unlike *Youngblood*'s "negligent" failure to refrigerate evidence, here the Government possessed actual knowledge that the destroyed evidence would prove innocence in a case alleging no legitimate services were delivered. Their own investigative materials document service delivery, yet they destroyed access to comprehensive proof of such delivery while falsely representing technical impossibility.

The *Youngblood* Court specifically noted that bad faith must be determined based on "the police's knowledge of the exculpatory value of the evidence at the time it was lost or destroyed." Here, the Government's grand jury presentation proves they knew the encrypted devices would contain evidence directly contradicting their prosecution theory--evidence showing systematic legitimate service delivery rather than fraudulent schemes.

This documented knowledge of exculpatory value, combined with selective evidence destruction, consciousness of guilt behaviors, and systematic deception to conceal the destruction, establishes the precise type of bad faith conduct that *Arizona v. Youngblood* prohibits and transforms this case from potentially "useful" evidence to clearly exculpatory material that the Government knew would undermine their entire prosecution theory.

4. Sixth Amendment Right to Defense Nullified

The Government's evidence destruction constitutes a fundamental violation of Mr. Aikens's Sixth Amendment right to present a complete defense. This right encompasses multiple interrelated protections that have been systematically violated here.

a. The Fundamental Right to Present a Defense

In *Rock v. Arkansas*, the Supreme Court established that criminal defendants possess a fundamental constitutional right to testify and present evidence in their own defense, rooted in multiple constitutional provisions:

"Criminal defendants have a right to testify on their own behalf under the Due Process Clause of the Fourteenth Amendment, the Compulsory Process Clause of the Sixth Amendment, and the Fifth Amendment's privilege against self-incrimination."

Rock v. Arkansas, 483 U.S. 44, 49-53 (1987). The Court emphasized that this right is essential to the adversarial system: "The right to offer the testimony of witnesses, and to compel their attendance, if necessary, is in plain terms the right to present a defense, the right to present the defendant's version of the facts as well as the prosecution's to the jury, so it may decide where the truth lies." *Washington v. Texas*, 388 U.S. 14, 19 (1967).

b. Arbitrary Restrictions Violate Constitutional Rights

The Supreme Court's decision in Rock established the foundational principle that "restrictions placed on a defendant's constitutional right to testify by a State's evidentiary rules may not be arbitrary or disproportionate to the purposes they are designed to serve." 483 U.S. at 53-56. The Government's destruction of evidence in this case creates precisely such an arbitrary and disproportionate barrier to the defendant's constitutional rights.

This case presents an even more egregious violation than Rock. While Arkansas in Rock imposed a facially neutral evidentiary rule that applied equally to all defendants, here the Government has manufactured an absolute evidentiary barrier through its own deliberate misconduct. The May 2, 2025 hearing revealed that Mr. Aikens cannot present essential evidence solely because the Government possessed the necessary access passwords for

over two years, then inexplicably destroyed or lost not only those passwords but also a MacBook hard drive and USB device containing critical evidence.

The Government cannot simultaneously serve as both the custodian of evidence and the architect of its destruction, then invoke that very destruction to bar the defendant's constitutional right to present a defense. Such conduct transforms evidentiary rules from neutral arbiters of relevance and reliability into instruments of prosecutorial advantage, creating the arbitrary and disproportionate restriction that Rock expressly prohibits.

c. The Right to Present Material Evidence

Washington v. Texas prohibits arbitrary rules that "prevent whole categories of defense witnesses from testifying on the basis of a priori categories that presume them unworthy of belief." 388 U.S. at 22. The Court emphasized that defendants must be able to present evidence that is "material and favorable to his defense." *Id.* at 16.

Here, the Government's evidence destruction prevents Mr. Aikens from presenting an entire category of evidence--comprehensive digital proof of legitimate business operations spanning multiple clients. As documented in Doc. 70-1, pages 426-428, this includes complete software development environments, client communications, financial related records, and video demonstrations of functioning deliverables.

d. Complete Nullification Rather Than Mere Limitation

The constitutional violation here exceeds the restrictions addressed in *Rock* and *Washington*. Those cases involved state rules that limited but did not eliminate defendants' ability to present evidence. Here, the Government's conduct has completely nullified Mr. Aikens's ability to present a complete technical evidence essential to his defense.

As Mr. Aikens testified at the May 2, 2025 hearing: "There's only one way to get into them, one way out. There's one key." Tr. 24. The Government destroyed that key while prosecuting Mr. Aikens for crimes the encrypted evidence would disprove.

e. No Legitimate Government Interest Justifies Destruction

Rock recognized that even fundamental rights may face limitations serving legitimate government interests, but held that such restrictions must be proportionate and not arbitrary. 483 U.S. at 56-62. Here, no legitimate government interest justified destroying Mr. Aikens's password systems. The Government's conduct violates basic evidence preservation protocols while claiming technical impossibility they created through their own negligence.

The Government's selective success in accessing the gaming computer using seized passwords--while claiming inability to access other devices containing exculpatory evidence--demonstrates the arbitrary nature of the restriction. This selective suppression violates the principle in *Washington* that defendants cannot be arbitrarily denied access to material evidence in their favor.

C. Schmid Factors Compel Dismissal as Only Adequate Remedy

1. Maximum Degree of Government Fault

The May 2, 2025 hearing established Government fault transcending negligence:

Systematic Protocol Violations:

- Violated mandatory FLETC RAM capture requirements
- Lost silver binder despite logging its seizure
- Lost USB device from same secure location
- Allowed MacBook hard drive to disappear entirely
- Maintained zero custody documentation

Pattern of Deception:

- July 2022: False promise of results "upon completion"
- February 2024: False representation of "45 to 60 days" needed
- Two years of maintaining fiction with no documented attempts
- Selective password use while claiming universal inaccessibility

2. Complete and Irreversible Prejudice

The prejudice represents total prevention of defense in a fraud case. The May 2, 2025 hearing established mathematical impossibility of proving innocence:

Technical Reality: Modern encryption cannot be broken without passwords. As Mr. Aikens testified regarding encrypted devices: "There's only one way to get into them, one way out. There's one key."[34]

Specific Prejudice: Mr. Aikens cannot show actual true time of alleged actionable deliverables in a case alleging no deliverables. The comprehensive evidence documented in Doc. 70-1 pages 426-428 spans:

- Complete software development environments across multiple clients
- Approvals and Computers showcasing and proving legitimate business operations
- Video demonstrations of functioning deliverables
- Client communications establishing satisfaction and delivery

No Possibility of Mitigation: Unlike physical evidence that might be partially recoverable, encrypted data without proper keys is permanently lost. The video evidence alone--spanning multiple functioning applications across Databases, Containers, iOS, Android, and web platforms--cannot be recreated through testimony alone.

3. No Lesser Sanction Can Remedy Constitutional Harm

Jury Instructions Are Wholly Inadequate: How does a jury evaluate invisible software? The May 2, 2025 hearing established specific technical evidence that instructions cannot address:

Mr. Melucci: "It would seem to me, if that was helpful to your case, you would want to see it and show it to the Court?"

Mr. Aikens: "Understandably, yes, but it requires the encryption -- it requires the encryption key."[35]

Evidence Suppression Is Insufficient: Suppressing Government evidence doesn't restore defense evidence. The Government retains witnesses while Mr. Aikens has encrypted devices he cannot access.

Deterrence Requires Meaningful Consequences: Lesser sanctions send dangerous messages that destroying evidence carries minimal consequences while defendants bear the burden of Government negligence.

D. Comparison to United States v. Miah

This Court's decision in *United States v. Miah* provides instructive contrast.[36] Every factor that defeated the spoliation claim in *Miah* supports finding spoliation here:

1. Control Element Distinction

Miah: Defendant controlled Twitter account and chose deletion before Government preservation was possible.

Aikens: Government had exclusive control of seized passwords and devices, with documented evidence of successful password use for some devices as established in the May 2, 2025 hearing.

2. Evidence Identification Contrast

Miah: Court noted Defendant "provides no specific examples of such content that he deleted."

Aikens: The May 2, 2025 hearing established specific identification of exculpatory evidence, reinforced by comprehensive documentation in Doc. 70-1 pages 426-428 spanning multiple business relationships.

3. Government's Systematic Destruction of Three Independent Access Methods

Unlike *Miah*'s technical impossibility, here the Government had complete custody and systematically destroyed three independent methods for accessing encrypted drives:

The Seized Papers: "Book storage media and papers listing passwords" containing 31 separate password sheets, documented in official logs, then lost from custody.

The USB Drive: Plaintext password exports seized from the same safe but vanished entirely.

The RAM Dump: Active password manager providing real-time access, destroyed by powering down rather than performing standard preservation procedures.

4. Government's Contradictory Success

The May 2, 2025 hearing revealed the Government successfully accessed "the gaming computer" using seized passwords while claiming inability to access other devices containing exculpatory evidence. This selective suppression distinguishes this case from *Miah*'s legitimate technical impossibility.

E. Judicial Estoppel Bars Government's Contradictory Positions

Judicial estoppel prevents parties from "prevailing in one phase of a case on an argument and then relying on a contradictory argument to prevail in another phase."[37]

The Government has taken irreconcilably **affirmative misrepresentations** that are inconsistent positions:

Position 1 (July 2022 - February 2024): "Forensic review ongoing, results will be provided upon completion"

Position 2 (May/June 2025): "Devices are encrypted and inaccessible after claiming passwords in hand oh and by the way we lost your binder, usb and macbook drive"

These positions are mutually exclusive. The May 2, 2025 hearing revealed the Government's selective success in accessing devices using seized passwords while maintaining claims of universal inaccessibility.

F. Complete Absence of Chain of Custody: Melendez-Diaz Violations

Melendez-Diaz v. Massachusetts established principles regarding documentary evidence in criminal prosecutions.[38] The complete absence of chain of custody documentation presents a fundamentally different issue than mere "gaps."

The May 2, 2025 hearing established we still don't know who handled what devices during crucial periods when evidence was being destroyed. No record exists of initial seizure procedures, custody transfers, storage conditions, or examination attempts.

This complete absence violates fundamental admissibility requirements and creates constitutional violations through inability to confront evidence handlers or authenticate Government claims about device condition.

CONCLUSION

This case presents a significant instance of government evidence loss or destruction in the digital era, characterized by substantial procedural failures spanning over two years. The evidentiary hearing of May 2, 2025 established that federal agents failed to follow established protocols for digital evidence preservation, resulting in the loss or destruction

of Mr. Aikens's password system through apparent negligence. Subsequently, the government maintained representations of "ongoing forensic review" when it knew or should have known that access to the evidence was impossible due to the aforementioned loss or destruction. Even more troubling, the government failed to conduct any verification of password functionality post-hearing and prior to Mr. Aikens's arrival, demonstrating a continued pattern of inadequate oversight and procedural compliance.

The evidence demonstrates systematic departures from standard evidence preservation procedures at every critical juncture, creating substantial and irreparable prejudice to the defense while raising serious questions about the integrity of the entire investigative process. These failures occurred across multiple stages of evidence handling, from initial seizure through attempted forensic examination, and were compounded by the government's inadequate disclosure to the defense and the Court regarding the true scope of the evidence loss or destruction. Despite the government's actual knowledge or constructive knowledge that such fundamental problems existed throughout the relevant time period, no corrective measures were undertaken, and misrepresentations about the status of evidence continued.

The cumulative effect of these failures extends beyond mere procedural violations, as they have fundamentally compromised the factual foundation of the government's case while denying the defense access to exculpatory evidence. The government's failure to implement basic safeguards for digital evidence preservation, use logical chain of custody and the like combined with its continued assertions regarding evidence availability despite knowing or having reason to know of the destruction and the ability to seek multiple times, represents a breakdown in the fundamental obligations owed to both the defense and the judicial system.

The Shocking Revelation

Until late 2024, Mr. Aikens reasonably relied on Government representations that they possessed the seized passwords and could access encrypted devices. Only when Mr.

Aikens actually asked HSI investigators to see the papers did they reveal the shocking truth: they only had a few scattered passwords, no silver binder existed in their custody, and critical evidence had vanished entirely then by the end of the meeting a macbook drive was missing and no USB in sight.

The Government seized the keys to Mr. Aikens's digital life and destroyed them. Their own evidence log and pictures documents seizure of password and the binder (USB) materials they now claim don't exist. Their selective success in accessing the gaming computer while claiming inability to access other devices exposes the pretextual nature of their "inaccessibility" claims.

Comprehensive Evidence Destruction

The record establishes destruction spanning multiple legitimate business relationships documented across Doc. 70-1 pages 426-428:

- **Complete software development environments** proving technical capability across multiple platforms
- **Video demonstrations** of functioning applications including iOS, Android, and web systems
- **Client communications** establishing satisfaction and delivery
- **Audio recordings** with actual client testimonials

All four *Bull v. UPS* spoliation elements are conclusively established:

1. **Control**: Complete Government custody with documented successful password access
2. **Relevance**: Proof of legitimate services in fraud case alleging none delivered
3. **Suppression**: Physical destruction of three independent password systems with selective concealment while in federal custody

4. **Foreseeability**: Mandatory constitutional preservation duties under Brady and FLETC training and their own Grand Jury presentation.

Constitutional Violations Requiring Dismissal

The *Schmid* factors compel dismissal as the only adequate remedy:

1. **Maximum Fault**: Systematic constitutional violations with consciousness of guilt behaviors
2. **Complete Prejudice**: Mathematical impossibility of proving innocence with no possibility of reconstruction
3. **No Lesser Sanction**: Constitutional harm cannot be remedied through instructions or evidence suppression

The May 2, 2025 hearing testimony established that Mr. Aikens cannot present crucial evidence essential to his defense. As the testimony revealed: "There's only one way to get into them, one way out. There's one key." The Government destroyed these keys while prosecuting Mr. Aikens for the very crimes the destroyed evidence would have disproven. Beyond Coleman's affirmative decision to turn off the PC, the Government lost the critical physical evidence that contained the passwords and access credentials—including papers and a USB drive that held the keys to other devices and cloud accounts, as well as a MacBook hard drive physically.

The Unprecedented Nature of Government Misconduct

The contrast with *United States v. Miah* is stark: where *Miah* involved legitimate technical impossibility, this case involves Government destruction of evidence in their exclusive custody combined with selective access and systematic deception. The Government's contradictory positions warrant judicial estoppel, and their complete failure to maintain chain of custody documentation violates fundamental *Melendez-Diaz* principles.

When the Government destroys a defendant's ability to prove innocence while prosecuting for crimes the destroyed evidence would disprove, fundamental constitutional principles require dismissal. The Government cannot benefit from evidence destruction of their own making while denying a citizen the right to present a complete defense.

The unprecedented scope of evidence destruction here—spanning multiple business relationships with comprehensive video proof of legitimate deliverables—creates precisely the constitutional violation that requires dismissal as the only adequate remedy.

For the foregoing reasons,

The irretrievable destruction of this critical evidence has fatally undermined Mr. Aikens' constitutional right to present an effective defense. The government's failure to preserve essential exculpatory material constitutes such a fundamental violation of due process that no remedy other than dismissal with prejudice can restore the integrity of these proceedings or cure the prejudice suffered by the defendant.

Dismissal with prejudice is not only warranted but necessary under these circumstances. The destroyed evidence was uniquely positioned to establish Mr. Aikens' innocence and cannot be reconstructed or replaced through any alternative means. No lesser sanction—including jury instructions, evidentiary presumptions, or monetary sanctions—can adequately address the constitutional violation or restore the evidentiary balance that existed prior to the destruction. The government's conduct has rendered a fair trial impossible, transforming these proceedings into a fundamentally unfair proceeding where the defendant has been stripped of his most potent defense tools.

Accordingly, dismissal with prejudice represents the only remedy that can vindicate Mr. Aikens' constitutional rights, deter future governmental misconduct, and preserve the integrity of the judicial system. To proceed with trial under these circumstances would

perpetuate the constitutional violation and deny Mr. Aikens the fair proceedings guaranteed by the Due Process Clause.

Footnotes:

[1] Doc. 76.

[2] *Id.*

[3] Tr. 15:3-4, May 2, 2025 Hearing.

[4] Digital Forensics Examiner Program, Fed. Law Enforcement Training Ctrs., https://www.fletc.gov/digital-forensics-examiner-program (last visited July 22, 2025).

[5] *Id.* ("The Digital Forensics Examiner Program (DF-E), formerly Seized Computer Evidence Recovery Specialist (SCERS), is a ten (10) day training program which teaches fundamental forensic analysis techniques... Students will conduct RAM capture analysis...").

[6] Letter from David J. Coleman, Computer Forensics Special Agent, HSI Pittsburgh, to Hon. W. Scott Hardy (Feb. 18, 2025), Case 2:22-cr-00119-WSH Document 67-8.

[7] Response from Joseph Soeka, Senior Digital Investigative Analyst, DOJ Cybercrime Laboratory (Apr. 30, 2025), Case 2:22-cr-00119-WSH Document 74-1.

[8] *Id.* at 1.

[9] Digital Forensics Examiner Program, Federal Law Enforcement Training Centers, https://www.fletc.gov/digital-forensics-examiner-program. (last visited July 22, 2025).

[10] Tr. 11, May 2, 2025 Hearing.

[11] ECF No. 70, p. 12.

[12] Tr. 10, May 2, 2025 Hearing.

[13] Tr. 16-17, May 2, 2025 Hearing.

[14] Defense Ex. C, IS-0000634953.

[15] Tr. 12, May 2, 2025 Hearing.

[16] Tr. 19, May 2, 2025 Hearing.

[17] Tr. 23-24, May 2, 2025 Hearing.

[18] Doc. 67-4.

[19] Feb. 21, 2024 Tr. 7:17-23.

[20] Tr. 31:24-32:7, May 2, 2025 Hearing.

[21] ECF No. 67, pp. 2-3, 21-22.

[22] Tr. 23, May 2, 2025 Hearing.

[23] *Bull v. United Parcel Service, Inc.*, 665 F.3d 68, 73 (3d Cir. 2012).

[24] *Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994).

[25] *Brady v. Maryland*, 373 U.S. 83, 87 (1963).

[26] *Rochin v. California*, 342 U.S. 165, 172 (1952).

[27] *California v. Trombetta*, 467 U.S. 479, 485 (1984).

[28] ECF No. 70, pp. 6, 14-15.

[29] *Berger v. United States*, 295 U.S. 78, 88 (1935).

[30] *Culler v. Shinseki*, No. 1:09-CV-0794, 2010 WL 5387084 (M.D. Pa. Dec. 22, 2010).

[31] *Zubulake v. USB Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2004).

[32] *United States v. Miah*, Criminal No. 21-110 (W.D. Pa. Nov. 29, 2021).

[33] Tr. 12, May 2, 2025 Hearing.

[34] Defense Ex. C, IS-0000634953.

[35] Tr. 23-24, May 2, 2025 Hearing.

[36] Tr. 19, May 2, 2025 Hearing.

[37] Tr. 31, May 2, 2025 Hearing.

[38] Tr. 11-12, May 2, 2025 Hearing.

[39] Tr. 24, May 2, 2025 Hearing.

[40] *United States v. Miah*, Criminal No. 21-110 (W.D. Pa. Nov. 29, 2021).

[41] *New Hampshire v. Maine*, 532 U.S. 742, 749 (2001).

[42] *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009).

[43] Rock v. Arkansas, 483 U.S. 44 (1987).

[44] Washington v. Texas, 388 U.S. 14 (1967).